

(a) Facility Security Officer Training. Licensees and others are responsible for ensuring that the Facility Security Officer, and others performing security duties, complete security training deemed appropriate by the CSA. Training requirements must be based on the facility's involvement with classified information and may include a Facility Security Officer orientation course and, for Facility Security Officers at facilities with safeguarding capability, a Facility Security Officer Program Management Course. Training, if required, should be completed within 1 year of appointment to the position of Facility Security Officer.

(b) Government-Provided Briefings. The CSA is responsible for providing initial security briefings to the Facility Security Officer, and for ensuring that other briefings required for special categories of information are provided.

(c) Temporary Help Suppliers. A temporary help supplier, or other contractor who employs cleared individuals solely for dispatch elsewhere, is responsible for ensuring that required briefings are provided to their cleared personnel. The temporary help supplier or the using licensee or other facility may conduct these briefings.

(d) Classified Information Nondisclosure Agreement (SF-312). The SF-312 is an agreement between the United States and an individual who is cleared for access to classified information. An employee issued an initial access authorization must, in accordance with the requirements of §25.23 of this chapter, execute an SF-312 before being granted access to classified information. The Facility Security Officer shall forward the executed SF-312 to the CSA for retention. If the employee refuses to execute the SF-312, the licensee or other facility shall deny the employee access to classified information and submit a report to the CSA. The SF-312 must be signed and dated by the employee and witnessed. The employee's and witness' signatures must bear the same date.

(e) Initial Security Briefings. Before being granted access to classified information, an employee shall receive an initial security briefing that includes the following topics:

- (1) A Threat Awareness Briefing.
- (2) A Defensive Security Briefing.
- (3) An overview of the security classification system.
- (4) Employee reporting obligations and requirements.
- (5) Security procedures and duties applicable to the employee's job.
- (f) *Refresher Briefings.* The licensee or other facility shall conduct refresher briefings for all cleared employees every 3 years. As a minimum, the refresher briefing must reinforce the information provided during the initial briefing and inform employees of appropriate changes in security regulations. This requirement may be satisfied by use of audio/video materials and/or by issuing written materials.
- (g) *Debriefings.* Licensee and other facilities shall debrief cleared employees at the time of termination of employment (discharge, resignation, or retirement); when an employee's access authorization is terminated, suspended, or revoked; and upon termination of the Facility Clearance.
- (h) Records reflecting an individual's initial and refresher security orientations and security termination must be maintained for three years after termination of the individual's access authorization.

[62 FR 17694, Apr. 11, 1997, as amended at 64 FR 15652, Apr. 1, 1999]

§95.34 Control of visitors.

(a) *Uncleared visitors.* Licensees, certificate holders, or others subject to this part shall take measures to preclude access to classified information by uncleared visitors.

(b) *Foreign visitors.* Licensees, certificate holders, or others subject to this part shall take measures as may be necessary to preclude access to classified information by foreign visitors. The licensee, certificate holder, or others shall retain records of visits for 5 years beyond the date of the visit.

[64 FR 15652, Apr. 1, 1999]

CONTROL OF INFORMATION

§95.35 Access to matter classified as National Security Information and Restricted Data.

(a) Except as the Commission may authorize, no person subject to the regulations in this part may receive or may permit any individual to have access to matter revealing Secret or Confidential National Security Information or Restricted Data unless the individual has:

(1)(i) A “Q” access authorization which permits access to matter classified as Secret and Confidential Restricted Data or Secret and Confidential National Security Information which includes intelligence information, CRYPTO (*i.e.*, cryptographic information) or other classified communications security (COMSEC) information, or

(ii) An “L” access authorization which permits access to matter classified as Confidential Restricted Data and Secret and Confidential National Security Information other than that noted in paragraph (a)(1)(i) of this section except that access to certain Confidential COMSEC information is permitted as authorized by a National Communications Security Committee waiver dated February 14, 1984.

(2) An established “need-to-know” for the matter (See Definitions, §95.5).

(3) NRC-approved storage facilities if classified documents or material are to be transmitted to the individual.

(b) Matter classified as National Security Information or Restricted Data shall not be released by a licensee or other person subject to part 95 to any personnel other than properly access authorized Commission licensee employees, or other individuals authorized access by the Commission.

(c) Access to matter which is National Security Information at NRC-licensed facilities or NRC-certified facilities by authorized representatives of IAEA is permitted in accordance with §95.36.

[59 FR 48975, Sept. 23, 1994]

§95.36 Access by representatives of the International Atomic Energy Agency or by participants in other international agreements.

(a) Based upon written disclosure authorization from the NRC Division of Nuclear Security that an individual is an authorized representative of the International Atomic Energy Agency (IAEA) or other international organization and that the individual is authorized to make visits or inspections in accordance with an established agreement with the United States Government, a licensee, certificate holder, or other person subject to this part shall permit the individual (upon presentation of the credentials specified in §75.7 of this chapter and any other credentials identified in the disclosure authorization) to have access to matter classified as National Security Information that is relevant to the conduct of a visit or inspection. A disclosure authorization under this section does not authorize a licensee, certificate holder, or other person subject to this part to provide access to Restricted Data.

(b) For purposes of this section, classified National Security Information is relevant to the conduct of a visit or inspection if—

(1) In the case of a visit, this information is needed to verify information according to §75.13 of this chapter; or

(2) In the case of an inspection, an inspector is entitled to have access to the information under §75.42 of this chapter.

(c) In accordance with the specific disclosure authorization provided by the Division of Nuclear Security, licensees or other persons subject to this part are authorized to release (*i.e.*, transfer possession of) copies of documents that contain classified National Security Information directly to IAEA inspectors and other representatives officially designated to request and receive classified National Security Information documents. These documents must be marked specifically for release to IAEA or other international organizations in accordance with instructions contained in the NRC’s disclosure authorization letter. Licensees and other persons subject to this part may also forward these documents